



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,228	11/26/2003	Marco Sasselli	3829-020-27	9959

24510 7590 06/18/2007  
DLA PIPER US LLP  
ATTN: PATENT GROUP  
1200 NINETEENTH STREET, NW  
WASHINGTON, DC 20036

EXAMINER
----------

REZA, MOHAMMAD W

ART UNIT	PAPER NUMBER
----------	--------------

2136

MAIL DATE	DELIVERY MODE
-----------	---------------

06/18/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>		<b>Applicant(s)</b>	
	10/721,228		SASSELLI ET AL.	
	<b>Examiner</b>		<b>Art Unit</b>	
	Mohammad W. Reza		2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 29 March 2007.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-18 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-18 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

1. This is in response to the arguments filed on 03/29/2007.
2. Claims 1-18 are pending in the application.
3. Claims 1-18 have been rejected.

***Response to Amendment***

4. The examiner approves the amendments made to Claims 1-14.
5. The examiner approves addition of new of Claims 15-18.

***Response to Arguments***

6. Applicant's arguments with respect to claims 1-18 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 1-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over James A. Sutton hereafter Sutton (Patent publication 20030196096) in view of Bantz et al hereafter Bantz (US Patent 7174017).

8. As per claim 1, Sutton discloses a method comprising the steps of: selecting by means of the apparatus key from a list of public keys stored in a non-volatile memory of the apparatus (paragraphs, 0021, 0027), receiving and storing in the patch in a random access memory; receiving the encrypted control block decrypting the encrypted control block using the selected public key, verifying that the decrypted control block corresponds to said patch data, installing the patch data (paragraphs, 0013-0014, 0026). Although, Sutton discloses a particular public key used for decryption (paragraphs, 0013-0014, 0021) and different patches need different keys to decrypt the patch data (paragraphs, 0025), he does not explicitly disclose the public key is the current public key, and deactivating the current public key such that a different public key is used to decrypt a next control block. Nevertheless, it is well known in the network security art at the time of invention that different keys require to decrypt different patch data is explaining the technology of deactivating the current decrypting key and use the new key for decrypting the new patch data. Exemplary of this is Bantz who discloses deactivating the current public key such that a different public key is used to decrypt a next control block (col. 3, lines 30-37).

Accordingly, it would be obvious to one of ordinary skill in the network security art at the time of invention was made to have incorporated Bantz's teachings of decrypting system for encrypting audio with the teachings of Sutton, for the purpose of suitably using the new decrypting key for decrypting the patch data properly (col. 2-4).

9. As per claim 2, Sutton discloses the Method wherein the control block includes a signature on the patch data, this signature being the result of a hash function (paragraphs, 0013-0014, and 0026).
10. As per claim 3, Sutton discloses the method wherein the verification of the block includes the step of establishing the signature on the received patch and the comparison with the decrypted signature in the control block (paragraphs, 0030-0031).
11. As per claim 4, Sutton discloses the method wherein the control block includes a symmetrical session key determined by the managing center, this key being used to encrypt the patch data (paragraphs, 0021, 0027).
12. As per claim 5-7, Sutton discloses the method wherein, for each update, a new public key taken from the list is used by the apparatus, wherein the public key is deleted from the list after being used, said key being useless for the next updates, and wherein the public keys of the list are used sequentially in a predetermined order during each update (paragraphs, 0021, 0027).
13. As per claim 8, Sutton discloses the method wherein the list of public keys is stored in a non-volatile memory, a key used for an update is definitively deleted from the memory that authorizes the access to the next key for the subsequent update (paragraphs, 0014).
14. As per claim 9, Sutton discloses the method wherein, for the updating of the software of an apparatus of a an old version to a new version, with a difference between the new version and the old version being greater than one, at least one message encrypted with a private key is added allowing the changing of the current key to the

next key in the list, the successful decryption of said message inducing the deactivation of the current key and the selection of the next key (paragraphs, 0021; 0027).

15. As per claim 10, Sutton discloses the method wherein the number of messages corresponds to the number of updates separating the initial version of the apparatus and the final version of the update (paragraphs, 0013-0014, and 0026).

16. As per claim 11, Sutton discloses the method wherein an updating installation is followed by an increment on a counter or by moving a pointer indicating the position of the key to be selected from the list during the subsequent update, while the list of keys remains unchanged (paragraphs, 0021, 0027).

17. As per claim 12, Sutton discloses the method according, wherein the control block is successively encrypted by the keys of the previous updates, each key from the list being used one after the other to decrypt the signature (paragraphs, 0030-0031).

18. As per claim 13, Sutton discloses the method wherein the apparatuses consist of Pay-TV decoders, an update of a decoder being carried out by downloading, from a managing center, of a patch accompanied by a control block, said block is stored in a Random Access Memory, and is decrypted with a current public key contained in a first non-volatile memory of the decoder, then verified and in the case of correspondence, a command leads the installation of the patch in a second non-volatile memory and the deactivation of the current key (paragraphs, 0021, 0027).

19. As per claim 14, Sutton discloses the method wherein a new list of public keys is transmitted to the decoder, said list replaces the list contained in the first memory containing keys deactivated by previous successful updates (paragraphs, 0021, 0027).

20. As per claim 15, Sutton discloses a system comprising: a processor; and a non-volatile memory connected to the processor for storing a list of public keys (paragraphs, 0021, 0027); wherein the processor is configured to perform the steps of receiving the patch data; receiving an encrypted control block associated with the patch data, the encrypted control block being encrypted with an asymmetrical private key selected from a list of keys in a management center; selecting a public key from the list of public keys stored in the non-volatile memory; decrypting the encrypted control block using the key selected in the previous step; verifying that the control block corresponds to the patch data; installing the patch data if the encrypted control block corresponds to the patch data stored and key stored in the non-volatile memory (paragraphs, 0013-0014, 0026). Although, Sutton discloses a particular public key used for decryption (paragraphs, 0013-0014, 0021) and different patches need different keys to decrypt the patch data (paragraphs, 0025), he does not explicitly disclose the public key is the current public key, and deactivating the current public key such that a different public key is used to decrypt a next control block. Nevertheless, it is well known in the network security art at the time of invention that different keys require to decrypt different patch data is explaining the technology of deactivating the current decrypting key and use the new key for decrypting the new patch data. Exemplary of this is Bantz who discloses deactivating the public key used in the decrypting step such that a new public key from the list of public keys (col. 3, lines 30-37).

The same motivation that was utilized in the combination of claim 1 applies equally as well to claim 14.

Art Unit: 2136

21. As per claim 16-18, Sutton discloses the system wherein the memory is an electrically erasable programmable read only memory (EEPROM), wherein the control block includes a signature on the patch data, the signature being a result of a hash function, wherein the control block includes a symmetrical session key determined by the managing center, the symmetrical session key being used to encrypt the patch data (paragraphs, 0013-0014, 0026).

### ***Conclusion***

22. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Art Unit: 2136

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mohammad w. Reza whose telephone number is 571-272-6590. The examiner can normally be reached on M-F (9:00-5:00).

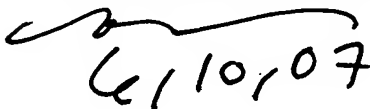
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **MOAZZAMI NASSER G** can be reached on (571)272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mohammad Wasim Reza

AU 2136

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100



6/10/07